Pearson BTEC Level 3 Nationals Diploma, Extended Diploma

Information Technology

Unit 11: Cyber Security and Incident Management

Part B

Sample assessment material for first teaching September 2017

Supervised hours: 4 hours

Paper Reference

20158K

You will need:
Forensic_Analysis.rtf

Instructions

- **Part A** and **Part B** contain material for the completion of the set tasks under supervised conditions.
- There are 43 marks for **Part A** and 37 marks for **Part B**, giving a total mark for the set task of 80.
- **Part A** and **Part B** are specific to each series and this material must be issued only to learners who have been entered to take the tasks in the specified series.
- This booklet should be kept securely until the start of the 4-hour, **Part B** supervised assessment period.
- **Part A** will need to have been completed and kept securely before starting **Part B**.
- Both parts will need to be completed during the 3-week period timetabled by Pearson.
- **Part A** and **Part B** tasks must be submitted together for each learner.
- **Part A** materials must not be accessed during the completion of **Part B**.
- This booklet should not be returned to Pearson.
- Answer **all** activities.

Information

- The total mark for this paper is 37.

Turn over ▶

S54093A

©2017 Pearson Education Ltd.

1/1/1/1/1/1/1/1/1/1/1

S 5 4 0 9 3 A

Pearson

Instructions to Teachers/Tutors and/or Invigilators

This paper must be read in conjunction with the unit information in the specification and the *BTEC Nationals Instructions for Conducting External Assessments (ICEA)* document. See the Pearson website for details.

Refer carefully to the instructions in this task booklet and the *Instructions for Conducting External Assessments (ICEA)* document to ensure that the assessment is supervised correctly.

Part A and **Part B** set tasks should be completed during the period of three weeks timetabled by Pearson. **Part A** must be completed before starting **Part B**.

The 4-hour, **Part B** set task must be carried out under supervised conditions.

The set task can be undertaken in more than one supervised session.

An electronic template for activity 4 is available on the website for centres to download for candidate use.

Learners must complete this task on a computer using the templates provided and appropriate software. All work must be saved as PDF documents for submission.

Teachers/tutors may clarify the wording that appears in this task but cannot provide any guidance in completion of the task.

Teachers/tutors and invigilators should note that they are responsible for maintaining security and for reporting issues to Pearson.

Maintaining Security

- Learners must not bring anything into the supervised environment or take anything out.
- Centres are responsible for putting in place appropriate checks to ensure that only permitted material is introduced into the supervised environment.
- Internet access is not permitted.
- Learner's work must be regularly backed up. Learners should save their work to their folder using the naming instructions indicated in each activity.
- During any permitted break, and at the end of the session, materials must be kept securely and no items removed from the supervised environment.
- Learners can only access their work under supervision.
- User areas must only be accessible to the individual learners and to named members of staff.
- Any materials being used by learners must be collected in at the end of each session, stored securely and handed back at the beginning of the next session.
- Following completion of **Part B** of the set task, all materials must be retained securely for submission to Pearson.
- **Part A** materials must not be accessed during the completion of **Part B**.

Outcomes for Submission

Each learner must create a folder to submit their work. Each folder should be named according to the following naming convention:

[Centre #]_[Registration number #]_[surname]_[first letter of first name]_U11B

Example: Joshua Smith with registration number F180542 at centre 12345 would have a folder titled

12345_F180542_Smith_J _U11B

Each learner will need to submit 2 PDF documents, within their folder, using the file names listed.

Activity 4: activity4_incidentanalysis_[Registration number #]_[surname]_[first letter of first name]

Activity 5: activity5_securityreport_[Registration number #]_[surname]_[first letter of first name]

An authentication sheet must be completed by each learner and submitted with the final outcomes.

Instructions for Learners

Read the set task information carefully.

Plan your time carefully to allow for the preparation and completion of all the activities.

Your centre will advise you of the timing for the supervised period. It is likely that you will be given more than one timetabled session to complete these tasks.

Internet access is not allowed.

You will complete this set task under supervision and your work will be kept securely at all times.

You must work independently throughout the supervised assessment period and must not share your work with other learners.

Your teacher/tutor may clarify the wording that appears in this task but cannot provide any guidance in completion of the task.

Part A materials must not be accessed during the completion of **Part B**.

Outcomes for Submission

You must create a folder to submit your work. Each folder should be named according to the following naming convention:

[Centre #]_[Registration number #]_[surname]_[first letter of first name]_U11B

Example: Joshua Smith with registration number F180542 at centre 12345 would have a folder titled

12345_F180542_Smith_J _U11B

You will need to submit 2 PDF documents, within your folder, using the file names listed.

Activity 4: activity4_incidentanalysis_[Registration number #]_[surname]_[first letter of first name]

Activity 5: activity5_securityreport_[Registration number #]_[surname]_[first letter of first name]

You must complete an authentication sheet before you hand your work into your teacher/tutor.

Set Task Brief

Bankside College

Bankside College has 800 pupils, aged from 11 to 18. Built in 1876, the college building has been extended over the years with the addition of administrative offices and classrooms.

The IT and D&T departments have recently been updated and share a new technology block. Both departments have some new equipment and improvements have also been made to IT provision in the rest of the college. This includes the equipping of all staff and pupils with Android-based tablets.

The plan of the college is shown in **Figure 1**.

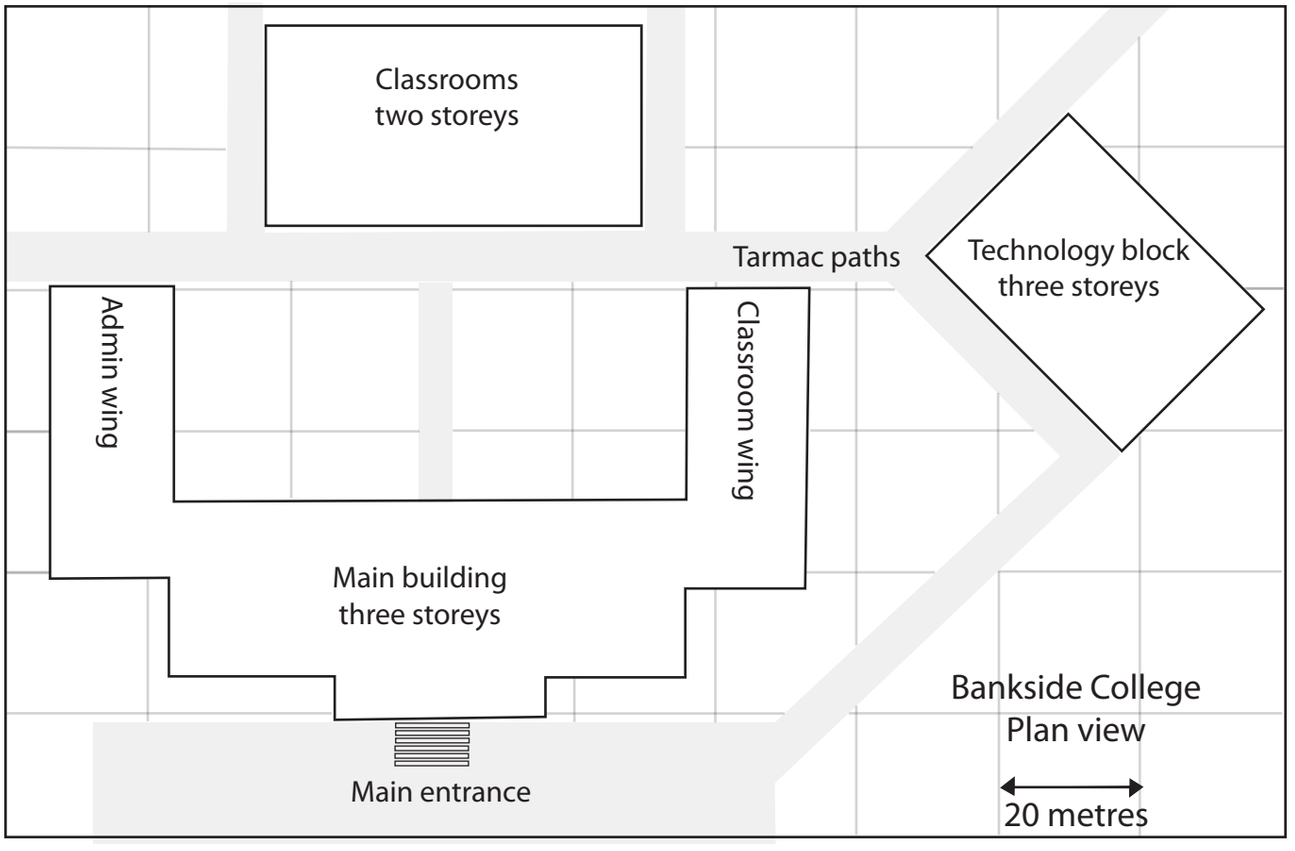


Figure 1

The Bankside College Local Area Network (LAN) has two sub-domains, Teaching and Admin. These have their own domain controllers, running Server 2016. The Admin domain controller is in the Administration wing, the Teaching domain controller is in the IT department. Each sub-domain has a Network Attached Storage (NAS) device and several networked printers.

The Teaching sub-domain services all of the computers used for teaching purposes, these run on Windows 8.1. All the tablets, regardless of use, are also serviced by the Teaching sub-domain, these run on Android 6 (Marshmallow). All users except network administrators are given a restricted user account.

The Admin sub-domain contains all other college computers. These include those in the administration offices, the staffroom, staff offices and anywhere else where computers

have been set up. The Admin computers vary in make, age and capability. They currently use a mix of Windows 10, 8.1, and 7. All users except network administrators are given a restricted user account.

Client brief

Last year you advised the Bankside College governors on network security when the college network was updated. It is now a year later and you have been asked to review the investigation of a cyber security incident.

Over the last few weeks, ransomware screens have been appearing on computers around the college. So far they have been restricted to classroom machines. None of the tablets have been affected.

The technicians carried out an investigation and identified the ransomware as being Javascript based. They have been able to remove it from affected machines. They were not able to trace its origin but have established that the software has been around for several years and tries to lock screens rather than encrypt files.

The governors have asked you to review the incident and the investigation that followed.

Evidence items from the security incident at Bankside College

Evidence items include:

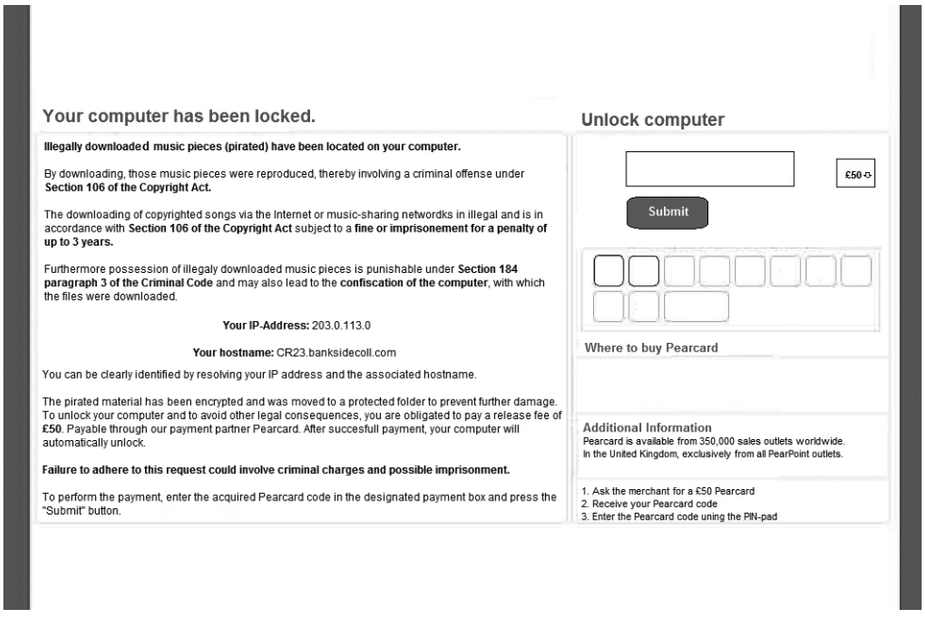
1 ransomware screenshot
2 the malware Javascript file
3 incident accounts
4 network diagram
5 cyber security document – incident management policy.

Evidence items 1 to 4 are required for Activity 4.

Evidence items 1 to 5 are required for Activity 5.

1. A screenshot of the ransomware

The technicians state that the screen takes over the browser. It cannot be resized or closed and will reopen immediately if the computer is shut down and restarted. The mouse pointer disappears, keyboard controls, to bring up Task Manager, for example, seem not to function and all taskbars, toolbars, etc. are hidden.



2. The malware Javascript file

```
<1 DOCTYPE html PUBLIC
<html xmnls="http://www.w3.org/1999/xhtml">
<script type="text/javascript" language="javascript">
var areYouReallySure = false;
var internalLink = false;
function areYouSure() {
if (!areYouReallySure && !internalLink) {
areYouReallySure = true;
str = 'YOUR BROWSER HAS BEEN LOCKED.\n\nILLEGALLY DOWNLOADED MUSIC HAS BEEN
FOUND ON YOUR COMPUTER.';
alert(str);
return str;
}
}
window.onbeforeunload = areYouSure;
</script>
```

3. Incident accounts

(a) College governor's recollection of events

The problem had been ongoing for a couple of weeks before it was brought up at a senior management meeting. It was then referred to the Project Management Committee, which had overseen the introduction of the new system.

The technicians had dealt with the immediate problem and worked out a way of recovering the locked computers without having to pay any ransom.

The technicians looked into the origins of the ransomware and found that it is a few years old. It works by locking the screen until payment is received and a release code is issued. It is essentially a browser exploit and only requires Javascript to be enabled for it to work.

We thought it odd that our anti-virus software did not pick it up, but concluded that someone must have altered the original ransomware to hide its signature.

The problem reoccurred several times over a period of about a month and then stopped. There are a number of theories about why, but the simplest explanation seems to be that the site or sites that were serving the script had been cleaned up.

The problem only manifested itself on classroom machines, so another possibility is that some pupils were visiting dubious sites and that they stopped once people began investigating the source of the infection.

(b) Technician's recollection of events

It began at the start of the summer term, 4th June. One of our pupils was searching for some images when the lock screen appeared. He could not say which website he was on, as he had simply clicked a link from an image search page.

I'd seen similar screens a few years ago, so knew how to fix it, but was puzzled by the fact that the anti-virus suite hadn't detected it. Clean up is fairly simple, we just reboot into recovery and perform a rollback to a previous restore point.

We then issued a general reminder about being careful when clicking on links. About a week later, we had another attack, then two more the next day. All were exactly the same screenlock. We were getting concerned as, the anti-virus still hadn't detected it. We checked each affected machine with a test file and that was picked up. The attacks reached double figures in the next week and then stopped. We haven't had any trouble since then.

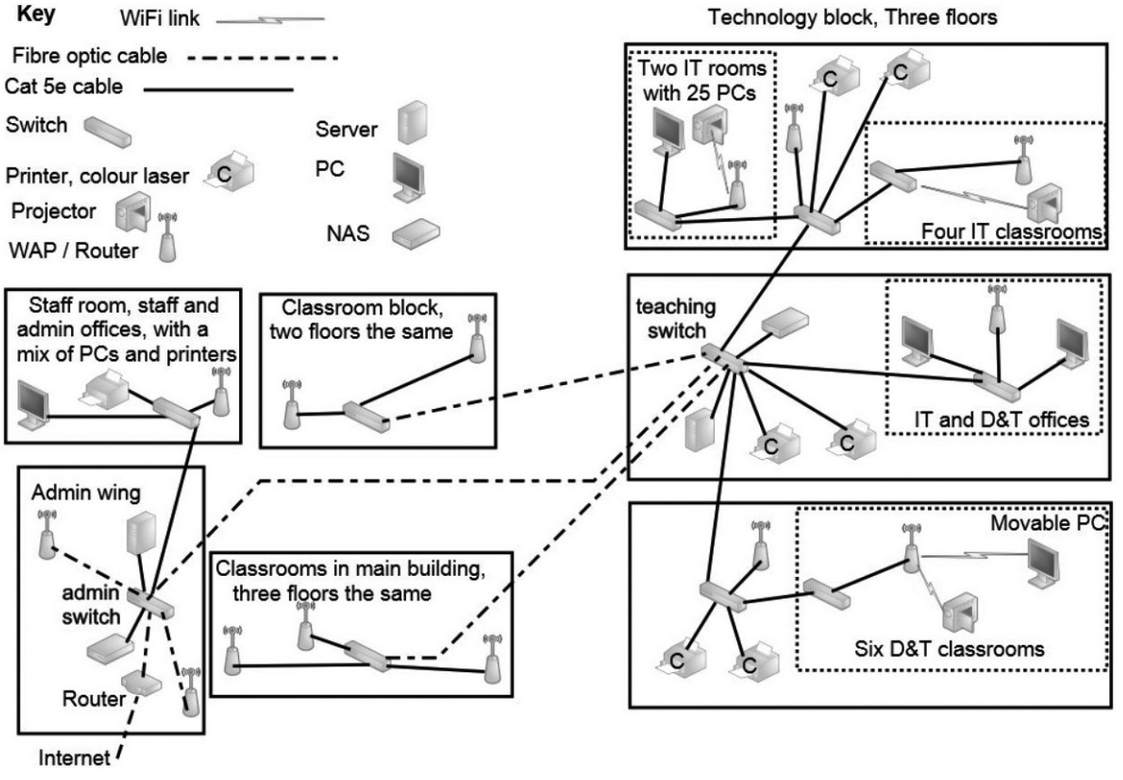
When we talked to the pupils affected by the screenlocks, they all said that they'd taken notice of our reminder and had been careful. They also said that the lock occurred on safe sites that they had visited previously. Two pupils claimed that they had been on an internal site maintained by the college chess club when it happened. We checked that site very carefully but found nothing. We also visited the external sites where they were known but nothing happened. It is impossible to determine if the claims about being infected from safe sites are true.

After the second week's attacks, we decided to have a close look at the affected machines. The rollback procedure may have removed any residual files but we thought it was worth taking a look.

We scanned for anything added between the start of term and the first attack. No malware turned up, but we found a file called HaHaHa.doc (**evidence item 2**). The file was located in the main Windows directory. It's a Javascript file but it was stored in doc format and therefore inert.

The file had been placed there on 3rd June and was owned by a senior member of staff who had required us to give him administrator access. He denied all knowledge of the file and had been out of college on that day. As a precaution, we imposed an immediate password change for all administrator level passwords and removed the file.

4. Network diagram



The first attack happened in one of the D&T rooms, the HaHaHa.doc file was on the same computer. Other attacks happened seemingly at random around the college, but always on classroom computers. No other computers were affected.

This evidence is only required for Activity 5.

5. Cyber Security Documentation – Incident Management Policy

Incident Management Team

The team shall consist of:

- the network manager (team leader)
- the senior IT technician
- the head of the IT department
- a member of the senior management team
- a college governor.

The senior management team member and governor will be designated and kept informed but will only take an active role if the incident is deemed serious.

Incident reporting

Any member of staff who considers that an IT-related security incident has occurred must report it as soon as possible to a member of the team. Initially it may be reported verbally but this must be followed up by a written / email account. It is the responsibility of the team to maintain documentation on the incident from first report to final resolution.

Security incidents may include:

- theft of IT equipment
- theft of college data
- unauthorised access to college IT systems
- infection of IT systems with malware
- physical incidents such as fire, flood, etc.

Incident response procedures

(a) Theft of IT equipment

- Theft of IT equipment is a very serious issue. Any thefts must be reported at once, providing as much information as possible (location and type of equipment, when it was last seen etc.)
- The team must ascertain if the item has actually been stolen (or if it has simply been moved or mislaid)
- If the item is confirmed as stolen the team leader must inform the senior management and governor members of the team, who will determine if the police need to be involved and who will run any internal enquiry
- The team must prepare a report on the theft for senior management and the governors.

(b) Theft of college data

- Theft or loss of college data may occur in a number of different ways
- Any loss or theft of data must be reported at once to the team leader
- The team must investigate the loss and identify exactly what data has been lost or stolen and when the incident occurred

- In the event that the data contains or may contain Personal Identifiable Information (PII), the team leader must inform the senior management and governor members of the team, who will determine if a breach of data protection laws may have occurred and who will run any internal enquiry
- Having identified what has been lost or stolen, the team must retrieve backups and restore the data as soon as possible
- The team should review the incident and implement procedures to prevent future losses.

(c) Infection of college IT systems with malware

- Any member of staff who suspects that any IT system has been compromised by malware must report the incident at once to a member of the team
- The infected system should be shut down as soon as possible
- The team will investigate the infection, and take appropriate measures to resolve the infection and restore the system
- In the event of a severe infection, which disrupts the day-to-day business of the college or which may cause a breach of data protection laws, the team leader must inform the senior management and governor members of the team, who will run any internal enquiry.

(d) Unauthorised access to college systems

- Any member of staff who suspects that there has been unauthorised access to any college IT system must report it at once to the team, providing as much detail as possible (which system, how access was obtained)
- The team will investigate the incident and identify how the unauthorised access was obtained
- The team will take whatever action is required to prevent future occurrences (change passwords etc.)
- Where the unauthorised access may breach data protection laws, the team leader must inform the senior management and governor members of the team, who will run the internal enquiry.

Part B Set Task

You must complete ALL activities in the set task.

Produce your documents using a computer.

Save your documents in your folder ready for submission using the formats and naming conventions indicated.

Read the set task brief carefully before you begin and note that reading time is included in the overall assessment time.

You have been advising the Bankside College governors on network security. Now, a year later, you have been called in to review the investigation of a cyber security incident.

Activity 4: Forensic incident analysis

Analyse the forensic evidence, including how the evidence was obtained, for the cyber security incident at Bankside College.

Consider possible causes of the incident and come to a conclusion about the most likely cause of the incident.

Refer to evidence items 1–4 inclusive.

Produce a forensic incident analysis using the template **Forensic_Analysis.rtf**

Save your completed forensic incident analysis as a PDF in your folder for submission as **activity4_incidentanalysis_[Registration number #]_[surname]_[first letter of first name]**

You are advised to spend 2 hours on this activity.

(Total for Activity 4 = 14 marks)

Activity 5: Security report

Review the incident. Suggest improvements and explain how they would prevent a similar incident in the future.

Areas for improvement are:

- adherence to forensic procedures
- the forensic procedure and current security protection measures
- the security documentation.

Read the set task brief and evidence items 1–5 inclusive when answering the question.

Save your completed security report as a PDF in your folder for submission as **activity5_securityreport_[Registration number #]_[surname]_[first letter of first name]**

You are advised to spend 2 hours on this activity.

(Total for Activity 5 = 20 marks)

(TOTAL FOR TECHNICAL LANGUAGE IN PART B = 3 MARKS)
TOTAL FOR PART B = 37 MARKS